

Notice of Allowability	Application No.	Applicant(s)
	09/827,697	MOREH ET AL.
	Examiner	Art Unit
	Philip B Tran	2155

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS. This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. This communication is responsive to interview on 3/1/2005 and 3/3/2005.
2. The allowed claim(s) is/are 1,4,8-22,25 and 29-41.
3. The drawings filed on 07 April 2001 are accepted by the Examiner.
4. Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
 - a) All
 - b) Some*
 - c) None
 of the:
 1. Certified copies of the priority documents have been received.
 2. Certified copies of the priority documents have been received in Application No. _____.
 3. Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

* Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.
6. CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
 - (a) including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
 - 1) hereto or 2) to Paper No./Mail Date _____.
 - (b) including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.
- Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).
7. DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. Notice of References Cited (PTO-892)
2. Notice of Draftsperson's Patent Drawing Review (PTO-948)
3. Information Disclosure Statements (PTO-1449 or PTO/SB/08),
Paper No./Mail Date _____
4. Examiner's Comment Regarding Requirement for Deposit
of Biological Material
5. Notice of Informal Patent Application (PTO-152)
6. Interview Summary (PTO-413),
Paper No./Mail Date Attached.
7. Examiner's Amendment/Comment
8. Examiner's Statement of Reasons for Allowance
9. Other _____.

KOSAIN ALAM

PRIMARY PATENT EXAMINER

EXAMINER'S AMENDMENT

1. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.
2. Authorization for this examiner's amendment was given in a telephone interview with Mr. Roberts (Reg. No. 38, 597), the undersigned on March 03, 2005.

The application has been amended as follows:

IN THE CLAIMS:

Cancel claims 2-3, 5-7, 23-24 and 26-28.

Replace claim 1 as follows:

-- 1. A system for authenticating a subject residing in a subject domain on a network to a server application residing in a server domain on the network, wherein a plurality of authentication mechanisms are present in an authentication domain on the network to affect the service provided by the server application, the system comprising:

a client for communicating with other components of the system and for authenticating the subject to other components of the system by providing client credentials on behalf of the subject, wherein said client also resides in the subject domain wherein the subject is selected from humans, client applications and applets;

an agent for communicating with other components of the system and for interacting said client to choose an appropriate authentication mechanism for the

subject from among the plurality of authentication mechanisms, wherein said agent resides in an agent domain on the network; and

a protocol proxy for communicating between said client and said appropriate authentication mechanism and for authenticating said client based on said client credentials, for obtaining from said appropriate authentication mechanism temporary credentials for said client to access the server application, and for creating from said temporary credentials an authentication name assertion allowing said client to access the server application.--

Replace claim 4 as follows:

-- 4. The system of claim 1, wherein said client interacts with said agent to determine a specification of said appropriate authentication mechanism and said client communicates said specification to said agent. --

Replace claim 8 as follows:

-- 8. The system of claim 1 wherein said agent includes a mechanism resolver for determining from the plurality of authentication mechanisms a subset of zero or more of the authentication mechanisms which affects the service provided by the server application. --

Replace claim 11 as follows:

-- 11. The system of claim 10, wherein said agent further includes a mechanism registrator for said appropriate authentication mechanism to register in said mechanism repository by adding information about itself. --

Replace claim 12 as follows:

-- 12. The system of claim 11, wherein said mechanism registrator is further for said appropriate authentication mechanism to update itself in said mechanism repository by changing information about itself.--

Replace claim 15 as follows:

-- 15. The system of claim 1, wherein said protocol proxy uses a standard security protocol to communicate with said client and a mechanism-specific protocol to communicate with said appropriate authentication mechanism. --

Replace claim 22 as follows:

-- 22. A method for authenticating a subject residing in a subject domain on a network to a server application residing in a server domain on the network, wherein a plurality of authentication mechanisms are present in an authentication domain on the network to affect the service provided by the server application, the method comprising the steps:

(a) gathering subject credentials for the subject and communicating said subject credentials to a protocol proxy;

(b) authenticating the subject to said protocol proxy with a client integrated into the subject by providing subject credentials on behalf of the subject, wherein the subject is selected from humans, client applications and applets;

(c) interacting between said client and an agent to chose an appropriate authentication mechanism for the subject from among the plurality of authentication mechanisms, wherein said agent resides in an agent domain on the network;

(d) obtaining a name assertion from said protocol proxy via said appropriate authentication mechanism which will allow said client to access the server application, thereby mediating between said protocol proxy and said appropriate authentication mechanism to permit the subject to access the server application via said client;

(e) creating an authentication name assertion with said protocol proxy based on said subject credentials which will allow said client to access the server application;

(f) communicating said authentication name assertion to said client; and

(e) communicating said authentication name assertion to the server application.--

Replace claim 25 as follows:

-- 25. The method of claim 22, further comprising:

interacting between said client and said agent to determine a specification of said appropriate authentication mechanism; and

communicating said specification with said client to said agent. --

Replace claim 29 as follows:

-- 29. The method of claim 22, further comprising:

(h) resolving from the plurality of authentication mechanisms a subset of zero or more of the authentication mechanisms which affects the service provided by the server application. --

Replace claim 30 as follows:

-- 30. The method of claim 29, wherein said agent further includes an authentication agent, and the method further comprising:

brokering between and authentication agent and said client in said step (h).--

Replace claim 31 as follows:

-- 31. The method of claim 29, wherein said agent domain further includes a mechanism repository, and the method further comprising:

storing information about said the plurality of the authentication mechanisms in said mechanism repository; and

querying said mechanism repository in said step (h). --

Replace claim 32 as follows:

-- 32. The method of claim 31, further comprising registering said appropriate authentication mechanism in said mechanism repository by adding information about said appropriate authentication mechanism. --

Replace claim 33 as follows:

-- 33. The method of claim 24, wherein said protocol proxy resides in said agent domain on the network. --

Replace claim 35 as follows:

-- 35. The method of claim 22, wherein said protocol proxy uses a standard security protocol to communicate with said client and a mechanism-specific protocol to communicate with said appropriate authentication mechanism. --

Allowable Subject Matter

3. Claims 1, 4, 8-22, 25, and 29-41 are allowed.

4. The following is an examiner's statements of reason for allowance:

Based on the amendment to claims 1, 4, 8, 11-12, 15, 22, 25, 29-33 and 35 and cancellation of claims 2-3, 5-7, 23-24 and 26-28 per interview with Mr. Roberts (Reg. 38,597) on March 03, 2005. The above mentioned claims are allowable over the prior art of record does not appear to teach or render obvious the claimed limitations in combination with the specific added limitations as recited in independent claims and subsequent dependent claims. The prior art of record fails to teach or suggest a method and system for authenticating a subject residing in a subject domain on a network to a server application residing in a server domain on the network wherein a plurality of authentication mechanisms are present an authentication domain on the network including authenticating the subject to other components of the system by providing client credentials on behalf of the subjects for interacting between agent and client to

choose an appropriate authentication mechanism for the subject from among the plurality of authentication mechanisms wherein the subjects is selected from humans, client applications and applets.

5. Pursuant to MPEP 606.01, the title has been changed to read:

-- A METHOD AND SYSTEM OF FEDERATED AUTHENTICATION SERVICE FOR
INTERACTING BETWEEN AGENT AND CLIENT AND COMMUNICATING WITH
OTHER COMPONENTS OF THE SYSTEM TO CHOOSE AN APPROPRIATE
MECHANISM FOR THE SUBJECT FROM AMONG THE PLURALITY OF
AUTHENTICATION MECHANISMS WHEREIN THE SUBJECT IS SELECTED FROM
HUMANS, CLIENT APPLICATIONS AND APPLETS --

6. Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the group receptionist whose telephone number is (703) 305-3900.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Philip B. Tran whose telephone number is (571) 272-3991.

mjam

HOSAIN ALAM
PATENT EXAMINER

Philip Tran
Philip B. Tran
Art Unit 2155
Mar 03, 2005